## DETAILED ACTION

In view of the Brief filed on September 17, 2009, PROSECUTION IS HEREBY REOPENED. A new rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446

### Status of Claims:

Claims 1-20 are pending in this Office Action.

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 4-11, 13-16, and 18-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Ginzboorg et al. (US 6,240,091 B1) hereinafter Ginzboorg.

### Claim 1

Ginzboorg teaches a data network management system for identifying unauthorized access to a data network service **(Column 15 Lines 40-44, "The charging functions correctly when the network access and payments are in synchronization with one another, i.e. when the paying customers have access to the network providing the services and the non-paying customers do not have access")**, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned**

**payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging”)**, said system comprising:

a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said node **(Column 15 Lines 44-50, “For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list”)**;

a database for maintaining an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node **(Column 15 lines 50-52, “and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network”)**; and

a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list and for updating said authorized access list, based on the user access list retrieved from said agent **(Column 15 lines 50-52, “If the address of a paying customer is not included in the access**

**list, the access server adds the address to the list. If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list. The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

**Claim 4**

Ginzboorg teaches the data network management system as defined in claim 1, further including means for installing said agent at said service node, said agent having means to communicate with said data communication means **(Column 5 lines 46-56, "FIG. 3a illustrates how the method according to the invention is applied in a network environment according to FIG. 2. The end user terminal (a personal computer) includes a smart card reader CR and each customer has a personal smart card by which the customer (subscriber) is recognized. Additionally, the terminal includes a program library which communicates with the smart card, and software which generates at specific intervals during the connection (for example, once a minute) a charging record furnished with a digital signature and sends it in the network")**.

**Claim 5**

Ginzboorg teaches a method for identifying unauthorized access to a data network service **(Column 15 Lines 40-44, "The charging functions correctly when the network access and payments are in synchronization with one another, i.e. when the paying customers have access to the network providing the services and the non-paying customers do not have access")**, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging")**, said method comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network **(Column 15 Lines 44-52, "For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation**

**the access server polls the router and the charging server. From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network")**;

b) comparing said user access list to an authorized access list; c) determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list **(Column 15 lines 50-52, "If the address of a paying customer is not included in the access list, the access server adds the address to the list. If an address included in the access list is not included in the paying customers of the charging server, the access server removes the address from the list. The polling interval can be made to be controllable so that the access service provider can set the desired interval")**;

d) if said access was not authorized, initiating a notification process; wherein said user access list identifies a plurality of accesses to said service node **(Column 18 lines 17-24, "The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging").**

## Claim 6

Ginzboorg teaches the method as defined in claim 5, further including updating said authorized access list based on said user access list retrieved from said service node **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging")**.

## Claim 7

Ginzboorg teaches method as defined in claim 5, further including installing said agent at said user node, prior to periodically polling and retrieving said user access list **(Column 5 lines 46-56, "FIG. 3a illustrates how the method according to the invention is applied in a network environment according to FIG. 2. The end user terminal (a personal computer) includes a smart card reader CR and each customer has a personal smart card by which the customer (subscriber) is recognized. Additionally, the terminal includes a program library which**

**communicates with the smart card, and software which generates at specific intervals during the connection (for example, once a minute) a charging record furnished with a digital signature and sends it in the network”)**.

## Claim 8

Ginzboorg teaches method as defined in claim 5, further including selecting said service node for identification based on a predetermined criteria, prior to retrieving said user access list **(Column 15 Lines 44-50, “For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list”)**.

## Claim 9

Ginzboorg teaches the method as defined in claim 5, wherein said notification process comprises notifying a Network Operations Console **(See claim 5 rejection “Access server”)**.

**Claim 10**

Ginzboorg teaches the method as defined in claim 5, wherein a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network **(Column 15 Lines 44-52, "For example, because of a fault the situation may sometimes change so that the router prevents the paying customers from accessing the network providing the services or allows access for non-paying customers (who do not send payment CDRs). To correct such a situation the access server polls the router and the charging server. From the router the access server gets the access list and from the charging server the IP addresses of the customers who pay at the moment in question for access to the network" and Column 15 lines 51-52, "The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

**Claim 11**

Ginzboorg teaches the method as defined in claim 5, wherein a) through d) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network **(Column 15 lines 51-52, "The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

**Claim 13**

Claim 13 is rejected for the same reasons as claim 5.

**Claim 14**

Ginzboorg teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of updating said authorized access list based on user access information **(Column 18 lines 14-24, "The router control unit RCU, which includes the router command set, controls the router by handling the maintenance of the aforementioned access list. The synchronization unit SU handles the synchronization of the aforementioned payments and access rights by comparing, at certain intervals, the router's list of open connections to addresses of paying customers. Said addresses are received from the charging server. Any detected conflicts are corrected so that no error longer than said interval can occur in charging")**.

**Claim 15**

Ginzboorg teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of installing said agent at said user node, prior to retrieving said user access list in step a) **(Column 5 lines 46-56, "FIG. 3a illustrates how the method according to the invention is applied in a network environment according to FIG. 2. The end**

**user terminal (a personal computer) includes a smart card reader CR and each customer has a personal smart card by which the customer (subscriber) is recognized. Additionally, the terminal includes a program library which communicates with the smart card, and software which generates at specific intervals during the connection (for example, once a minute) a charging record furnished with a digital signature and sends it in the network")**..

**Claim 16**

Ginzboorg teaches the computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions wherein said steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network **(Column 15 lines 51-52, "The polling interval can be made to be controllable so that the access service provider can set the desired interval")**.

**Claim 18**

Claim 18 is rejected for the same reasons as claim 1.

**Claim 19**

Ginzboorg teaches the data network as defined in claim 1, wherein said authorized access list is a common authorized user access list, that includes a range of user nodes for comparing to said user access list to determine if said user access list is a subset of said common authorization access list **(Column 9 lines 31-40, "This can be a drawback if the charging server and the access server belong to different organizations. This possible drawback can be "fixed" in the following manner. The customer identifier is formed of two parts. The first part identifies the customer origin (i.e. the customer's own charging server). This part is used to route the START message to the charging server in question. The second part is encrypted by using the public key of the customer's own charging server so that it is not recognized by the access server")**.

### Claim 20

Ginzboorg teaches the data network management system of claim 1 wherein said user access list identifies a plurality of accesses to said service node **(See claim 1 rejection)**.

### *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2-3, 12, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginzboorg in view of Noy et al. (US 6,539,540 B1).

**Claim 2**

Ginzboorg teaches the data network management system as defined in claim 1.

Ginzboorg does not specifically disclose wherein said agent is a Simple Network Management Protocol agent.

However, Noy et al. teaches in Column 1 line 30, “an SNMP manager will periodically poll an agent 30” in order to detect changes in information for a particular network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Ginzboorg to include “an SNMP manager will periodically poll an agent 30” as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

**Claim 3**

Ginzboorg teaches the data network management system as defined in claim 1.

Ginzboorg does not specifically disclose wherein said data communication means is a Simple Network Management Protocol communication means.

However, Noy et al. teaches in Column 1 line 30, "an SNMP manager will periodically poll an agent 30" in order to detect changes in information for a particular network device (Column 1 lines 31-32).

It would have been obvious to one of ordinary skill in the art at the time of invention to create the invention of Ginzboorg to include "an SNMP manager will periodically poll an agent 30" as taught by Noy in order to detect changes in information for a particular network device (Column 1 lines 31-32).

**Claim 12**

Claim 12 is rejected for the same reasons as claim 2.

**Claim 17**

Claim 17 is rejected for the same reasons as claim 2.

***Response to Arguments***

Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FARHAD ALI whose telephone number is (571)270-1920. The examiner can normally be reached on Monday thru Friday, 7:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Farhad Ali/
Examiner, Art Unit 2446

/Jeffrey Pwu/
Supervisory Patent Examiner, Art Unit 2446